PURPOSE

This transmits Chapter 3, Information Protection, of new Handbook 1.16.8, Physical Security Standards, which replaces IRM 1(16)41, Physical and Document Security Handbook.

BACKGROUND

The IRM is being converted to a new format and style which will be issued in 8½" x 11" instead of the current 6" x 9" size. The new IRM Handbook includes simplified text, a new numbering system, and a new format for organizing text.

The transmittal reissues existing information in the IRM format and provides new guidelines on facility, property and information protection. It replaces text currently contained in IRM 1(16)41 which is obsolete.

NATURE OF MATERIALS

New IRM Handbook 1.16.8, Physical Security Handbook, provides guidance and procedures for the protection of information, property and facilities.

Leland N. Keller
National Director, Real Estate
Planning and Management Division

Table of Contents

Chapter 3
Information Protection

3.1 (02/26/99)
Overview

(1) The protection of information is of vital concern to the Service. Every effort must be made to ensure that all documents are provided protection commensurate with the information therein.

(2) For the purpose of this Handbook the terms “tax data” and “tax information” include “return” and “return information” as defined in the Internal Revenue Code (IRC) 6103(b).

(3) In addition to tax data, there are many other documents that require protection from disclosure, such as Law Enforcement Manuals, informant communications, personnel files and employee medical records, investigator files, national security information (classified), security clearance files, employment testing materials, grand jury information, passwords, and proprietary information.

(4) Information such as training material, statistical files and various internal communications may require protection from disclosure and undesired dissemination. The manager of the function originating the information shall determine the degree of protection required, if any, and will work with the Security staff to implement appropriate protective measures.

(5) The sensitivity of information on media such as magnetic tapes or disks, microfilm, microfiche, etc. may not be readily apparent without the use of equipment. Therefore all Service personnel must take care to ensure they recognize information which requires protection regardless of the media on which that information is contained. For additional guidance on security of computer systems and magnetic media, see 2.10.0 (Automated Information Systems Security Manual).

3.2 (02/26/99)
Disclosure of Tax Information

(1) The Tax Reform Act of 1976 provides that returns and return information are to be confidential and not subject to disclosure except as specifically provided in IRC 6103, or other sections of the Internal Revenue Code. Internal Revenue Code 7213 and 7217 include civil and criminal penalties for willful or negligent disclosure of returns or return information.

(2) IRM 1.3, Disclosure of Official Information Handbook, contains guidelines governing the release of data included on tax returns and other information contained in Service files. Release of any tax data whether on microfilm or photocopy impressions to any other Federal or state government activity shall be effected in accordance with the disclosure requirements in IRC 6103 and IRM 1.3. The Disclosure office should be consulted on release of this type of information.

(3) In addition to guarding against unauthorized disclosure of tax information by Service employees, steps must be taken to prevent the possibility of such disclosure by non-Service personnel. Care must be taken to deny unauthorized non-Service personnel access to other than those areas which have been established for serving the public. All tax data in

nonsecured areas *must be containerized* during nonduty hours and *must be protected* from inadvertent disclosures during duty hours.

(4) Those individuals who have a “need to know”, such as certain government contractors and vendor personnel, must be informed of the protection requirements under the law. This can be best accomplished in writing, quoting the appropriate sections of 1(14)20 and citing the prohibitions, restrictions and penalties for unauthorized disclosure of tax return and return information under appropriate sections of the Internal Revenue Code.

3.2.1 (02/26/99)
Microfilm and Computer Output Data

(1) All magnetic media and computer output data containing tax data will be properly accounted for by the user. Requests (except telephonic requests) for research for tax data contained on microfilm or on computer output (e.g. IDRS) must be made on the appropriate forms. Custodians of tax information will assure themselves that persons requesting tax information by telephone are IRS employees. One way of obtaining this assurance is for the custodian to require the requestor’s manager to furnish a list of authorized callers which contains identifying information such as ID card numbers. The custodians may then require callers to identify themselves with specific information before furnishing the requested data. Another option is to develop a code system known only to the custodians and authorized callers. Still another option is for the custodians to furnish the requested information to a designated contact.

(2) To ensure that microfilm tax data and computer output data are properly accounted for, records of productions, transmissions, receipt, reproductions, location, storage and destruction will be maintained in accordance with IRM 2700.

3.2.2 (02/26/99)
Release of Tax Data Outside of IRS

(1) Release of any tax data, whether on microfilm or photocopy impressions to any other Federal or state government activity shall be effected in accordance with IRC 6103 and the Disclosure of Official Information Handbook (IRM 1.3), which contains instructions for periodic review of the safeguards of Federal tax returns and return information established by such agencies receiving this material. These reviews are required to meet the provisions of IRS 6103(p). Procedures for conducting safeguard reviews can be found in 1.16.3.

3.2.3 (02/26/99)
Protection of Informant Information

(1) The identity of persons who furnish information regarding possible tax violations, must be protected. All employees must, therefore, handle such information in strict confidence. Such information must be given special handling to avoid disclosure to other than those employees having an absolute “need to know.”

(2) As soon as informant correspondence is recognized by mail classifiers or other employees, it will be sealed in “To Be Opened by Addressee Only” envelopes and routed to the Criminal Investigation activity. These same

precautions will also apply to claims for rewards, memorandums of oral interviews with informants, or any other communications which might, in any way, identify informants.

(3) The routing of information communications to other activities by the Criminal Investigation activity will be made by transmission in sealed envelopes bearing instructions “To Be Opened by Addressee Only” or by handcarrying the material to the appropriate office.

(4) In order to maintain maximum security, informant communications claims for reward, claims for reward reports, memorandums or documents which identify informants will be afforded containerized protection at all times, except when such documents are being processed. Access to such storage containers will be limited to the person or persons responsible for the security of the documents.

3.2.4 (02/26/99)
State and Local Government Tax Returns

(1) State and local government tax returns and other non-Federal tax information will be protected in the same manner as the corresponding Federal tax return or tax information.

3.2.5 (02/26/99)
Other Protectable Information

(1) For other categories of protectable information, such as those protected under the Privacy Act, see the Disclosure of Official Information Handbook.

(2) Procedures for the Official Use only and Limited Official Use information are contained in 1.16.7.

(3) Information classified Top Secret, Secret or Confidential under Executive Order 12958 (Classified National Security Information) will be protected in accordance with 1.16.7, Safeguarding Documents and National Security Information Handbook. Although the Service rarely has had an occasion to classify a document containing National Security Information, it does have custody of some documents so classified. Complete instructions for handling, storing, transmitting and disposing of, as well as instructions for classifying an original document if it becomes necessary are contained in 1.16.7.

3.3 (02/26/99)
Storage, Handling Transmission and Disposition of Sensitive Information

(1) Sensitive information (including tax and tax-related information) is any information which if lost, stolen, or altered without proper authorization, may adversely affect Service operations. For example, unauthorized disclosure of an individual’s tax information may cause lawsuits against Service officials as well as the Service, unwanted notoriety for the Service, and public distrust in the Service’s ability to protect such information, all of which may result in an increase in noncompliance with tax laws. Unauthorized release of information such as the name and address of an informant may threaten that person’s life. The following requirements cover the most sensitive types of information only. Often,

the employee or manager working with sensitive information not mentioned herein will be able to determine how much protection is required and how that protection can best be provided.

3.3.1 (02/26/99)
Storage

(1) A document containing information that requires protection must be stored in accordance with minimum protection standards whenever it is not in the custody of an authorized IRS employee.

(2) Field employees, at times, have sensitive information at the taxpayer's site which should be stored at an IRS facility. Service managers must ensure that employees adequately secure such information at the taxpayer's site. Sensitive tax information, such as agent's workpapers, original returns, examination plans, probes, fraud data, etc. which is housed at the taxpayer's site, must be stored in a container under the control of the responsible Service employee. This container must be either a security container furnished by the Service, or if using a taxpayer furnished container, it must be modified by the Service (e.g., bars and locks) so that the Service is assured that the taxpayer cannot access the container. During duty-hours, the data must be under the personal custody of the Service employee if it is not containerized. If a lockable and suitable container cannot be provided, sensitive tax information will not be left at the taxpayer's site.

3.3.2 (02/26/99)
Handling

(1) The handling of tax and tax-related documents must be in such a manner that they do not become misplaced or available to unauthorized personnel. Only those employees who have a need to know will be permitted access to tax and tax-related information. Tax information will not be released outside the Service except as provided in the Internal Revenue Code.

(2) For protection from a casual observation (unauthorized) Document 6441, Special Cover Sheet, as revised may be used as a cover for all Law Enforcement Manuals (see section 3.4 of this Handbook).

3.3.3 (02/26/99)
Transmission

(1) Tax information transmitted from one location to another must be provided adequate safeguards. If a person handcarries the material in connection with a trip or in the course of daily activities, it should be kept with him/her to the extent possible. If tax information must be left in an automobile, it should be locked in the trunk. If the vehicle does not have a trunk the material should be concealed from plain view and secured in some manner. In either case, the vehicle should be locked and the material left unattended for only a short period. Hotel/motel rooms are usually not good locations to secure tax information; however, if the material must be left in such a location, it should be locked in a briefcase and concealed to the extent possible.

(2) All shipments of tax returns and return information (including magnetic media and microfilm) from any service center to the National Office,

regional offices, district offices, the Martinsburg or Detroit Computing Centers, or other agencies and other jurisdictions, will be documented on Form 3210, Document Transmittal, or similar form and monitored to ensure that each shipment is properly and timely received and acknowledged. Every Service office engaged in the shipment of tax returns and return information shall designate individuals to be responsible for monitoring the shipments. (Also see IRM 2700.)

(3) Form 3220, Mass Storage Media will be used for transmittal of all magnetic tape as specified in IRM 2700.

(4) Tax data being retired to Federal Records Centers will be transmitted with SF 135, Record Transmittal and Receipt. Column "f" of this form will contain the following statement:

"These are restricted records and must be guarded at all times from disclosure to unauthorized persons."

(5) Instructions provided in IRM 1.15.2, Chapter 22, Records Control Schedule for Service Centers will be followed for the packing and shipping of tax data and all shipments will be coded "W" to require both restricted access and witnessed destruction.

(6) Tax data transmitted to other authorized agencies and jurisdictions will be transmitted in accordance with this Handbook and recordkeeping requirements of IRM 1.3, Disclosure of Official Information Handbook. These instructions do not apply to tax data transmitted to foreign governments in accordance with tax treaties.

(7) Information covered with Document 6441 shall be double wrapped when transmitted from one Service facility to another. Pink Envelope E–19 or E–20 will be used as the inner wrapping. Any additional envelope, sealed mail bag or pouch, or sealed jiffy bag of the appropriate size will be used as the outer wrapping. If E–19 or E–20 cannot be used for an inner wrapping when transmitting covered information, the inner wrapping must be marked "TO BE OPENED BY ADDRESSEE ONLY."

3.3.4 (02/26/99)
Disposition and Destruction

(1) Disposition and destruction of tax information must be in accordance with the IRM 1.15.2 (Records Disposition Handbook). Although IRS employees may know the proper methods of destroying tax data, management must reinforce this knowledge by including document destruction as a topic in orientation sessions, periodic group meetings and other awareness sessions.

3.3.4.1 (02/26/99)
Disposition

(1) Waste material generated in the processing of tax documents, protected data or other related documents must be destroyed by burning, disintegrating, pulping, shredding or by any other manner which in the judgement of the responsible security official renders the information contained in such material irrecoverable. The fact that material has been

identified for destruction does not change the requirement to provide appropriate protective measures. Waste material must be provided the protection equal to that required by the most protected item. This material may include, but is not limited to, extra copies, photo impressions, microfilm, printouts, computer tape printouts, IDRS printouts, carbon paper, notes, workpapers or any other material containing tax information which has served its purpose. Disposition of magnetic media can be found in IRM 2.10.0.

3.3.4.2 (02/26/99)

Destruction Precautions

(1) The purpose of destroying tax information is to keep the information from being disclosed to unauthorized personnel. Protected information on any media will be removed, obliterated or the media destroyed by or in the presence of an IRS employee. Security personnel will work with managers to develop and implement local procedures to enhance the concepts outlined here.

(2) In the event tax information media is to be collected and destroyed by an independent contractor, to preclude the necessity of having an IRS employee present during destruction, the contract must include the safeguard provisions required by IRC 6103(n) and regulations thereunder. The provisions of the contract must allow for IRS inspection of the contractor facility and operations to ensure the safeguarding of IRS information. Waste material must be maintained in a secured container in a secured area to prevent sensitive information from unauthorized disclosure or access. The contractor must provide a certificate of destruction.

(3) Paper data will be destroyed in one of the following ways:

- shredding to effect 5/16 inch wide or smaller strips,
- pulping to be accomplished in such a manner that all material is reduced to particles one inch or smaller;
- disintegrating to be accomplished with ½ inch or smaller screen;
- burning to effect complete incineration.

(4) When it becomes necessary to store protected information which has been collected for destruction, it will be provided protection equal to that required by the most protected item. All tax data will be destroyed by or in the presence of an IRS employee or authorized contract employee.

(5) Microfilm will be returned to the service center for destruction by shredding to effect 1/35 inch by 3/8 inch strip. Microfilm in the National Office will be destroyed similarly by the National Office. (Service center destructors may be used for the destruction of microfilm if they meet the specifications.)

(6) Protected information contained on any other form of media will be removed, obliterated, or the media destroyed by or in the presence of an IRS employee or contractor employee in such a manner that the information is totally unrecoverable. For guidance on disposition of magnetic media, see IRM 2.10.0.

(7) After the protected information has been destroyed as specified in these standards, there are no restrictions on how or by whom the material will be collected and transported.

(8) To reduce the cost involved in destroying tax data, local procedures will be developed to prevent employees from throwing coffee cups, lunch bags, newspapers, etc., in receptacles reserved for protected information.

(9) There may be areas or activities where the volume of paper documents containing tax information is sufficient to make it more practical to destroy all documents in the area of activity.

3.3.4.3 (02/26/99)
Recycling

(1) The Service supports the recycling program. Documents containing tax information or other sensitive information may not be placed in regular recycling containers, but must be placed in secured containers and must be clearly marked.

(2) The preferred approach is that sensitive information be segregated and shredded in accordance with IRS guidelines (see 3.3.4.2 of this Chapter) prior to turning it over to the recycler.

(3) Unshredded sensitive information may be turned over to a contractor provided the contract includes necessary safeguards that will ensure compliance with 6103(n) requirements, provides for periodic safeguard reviews and includes language describing methods of collection, pick-up, storage and disposition. The contract should also include provisions for a Certificate of Destruction.

(4) Another method is to have IRS personnel observe the destruction of sensitive information upon delivery to the recycler. This allows for destruction of sensitive information while maintaining custody of the material up to the moment of destruction. Again the contractor must be in compliance with 6103(n) requirements which provides for safeguards and periodic safeguard reviews. However, this method is not recommended because of the resources that would be required.

3.4 (02/26/99)
Special Cover Sheet (Document 6441)

(1) Document 6441 may be used as a cover sheet for all Law Enforcement Manuals. It may be used as a cover sheet for any other information when the originator determines that written information should have special handling and other than normal storage.

(2) Document 6441 is designed to catch attention and remind employees that any information attached to the cover sheet is to be protected from disclosure. All persons not having a need to know the information in the performance of their official duties, are to be denied access to the covered information.

(3) When using the cover sheet, Exhibits 1.16.8.5–1 and 1.16.8.5–2 should be reviewed to determine the storage requirements for the information to

be covered. Space is provided on the cover sheet to enter the degree of storage required. For example, information from an informant, would require the entry “SP–2”. As can be noted in Exhibit 1.16.8.5–1, “SP–2” requires storage in a security container or security room.

3.5 (02/26/99)

Information Security During Office Moves

(1) When it is necessary for an office to move to another location, plans must be made to properly protect and account for all tax data and other information, as well as government property. The circumstances of the move must be carefully considered (e.g., the distance involved and the method to be used in making the move). Tax documents and other information will be kept in locked cabinets or sealed in packing cartons while in transit. Accountability will be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move. Throughout the move, classified material and other critical material will remain in the custody of an IRS employee with the appropriate clearance and need to know. The precautions taken to protect Government property during the move will be commensurate with the type and value of property involved. Small items of high value will be packed in cartons or moved in locked cabinets. Accountability will be maintained throughout the move.